Brasoftware®

Alexandre Nakano
Arquiteto de Soluções
t-Alexandre.Nakano@brasoftware.com.br

Brasoftware®
consulting

Microsoft 365 (Security) – Defender for Endpoint

Agenda:

- Solução Proposta;
- Escopo do Projeto;
- Requisitos do Ambiente / Premissas;
- Cronograma Macro, Recursos e Custos de Serviço

Solução Proposta

Implementação de setup de Segurança Microsoft para os produtos abaixo:

- ❑ Microsoft Defender for Endpoint

Escopo Macro

Microsoft 365

- ❑ **Iniciação**
- ❑ **Planejamento**
- ❑ **Microsoft Defender for Endpoint – P2**
  - ✓ Setup da instância do Microsoft Defender for Endpoint
  - ✓ Configuração Portal Microsoft Defender for Endpoint
  - ✓ Validar se os pontos de extremidade (dispositivos) estão se comunicando com o Portal do Defender for Endpoint
  - ✓ Delegar acesos aos administradores de segurança e operadores de segurança ao Defender for Endpoint
  - ✓ Habilitar o Microsoft Defender em até 10 estações Windows
  - ✓ Configurar o Microsoft Defender Antivírus para o modo passivo
    - ✓ Este modo é para que o antivírus atual e o Microsoft Defender Antivírus possam ser executados lado a lado até que seja concluído à integração com o Microsoft Defender para Endpoint.
  - ✓ Obter atualizações para o Microsoft Defender Antivírus
  - ✓ Adicionar o Microsoft defender para Endpoint à lista de exclusão do antivírus atual (responsabilidade cliente)
  - ✓ Adicionar o antivírus atual à lista de exclusão do Microsoft Defender Antivirus
  - ✓ Adicionar o antivírus atual à lista de exclusão do Microsoft defender para Endpoint

Escopo
Microsoft 365

- **Microsoft Defender for Endpoint – P1**
  - ✓ Configurar grupos de dispositivos, coleções de dispositivos e unidades organizacionais
  - ✓ Configurar políticas anti-malware e proteção em tempo real
  - ✓ Configuração de Detecção e investigação de alertas
  - ✓ Configurar métodos de integração do Defender for Endpoint
  - ✓ Executar testes de detecção
  - ✓ Acompanhar desinstalação do antivírus atual em até 10 estações Windows (responsabilidade cliente)
  - ✓ Realização do onboard de até 10 estações de trabalho Windows via Intune ou MECM ou GPO
  - ✓ Validar se o Microsoft Defender para Endpoint está no modo ativo
  - ✓ Testes e Validações do ambiente Defender for Endpoint
- **Finalização**
  - ✓ Estabilização do ambiente;
  - ✓ Repasse de conhecimento (workshop técnico);
  - ✓ Documentação Técnica Final

Escopo

Microsoft 365

- **Microsoft Defender for Endpoint – P2 (adicional)**
  - ✓ Configuração de MDfE File Investigation
  - ✓ Configuração de MDfE File-less Attack Investigation
  - ✓ Configuração de MDfE Machine Investigation
  - ✓ Configuração de MDfE Threat Analytics
  - ✓ Configuração de MDfE Threat & Vulnerability Management (TVM)
  - ✓ Configuração de MDfE Live Response
  - ✓ Testes e validações em até 10 estações de trabalho Windows

Requisitos do Ambiente / Premissas

Microsoft Defender for Endpoint

- Acesso global admin no Tenant de 365;
- Dispositivos com Windows 10 Enterprise / Educational mais recente ingressados no Azure Active Directory e gerenciados pelo Intune
- Nível funcional do Active Directory recomendado no mínimo Windows Server 2012 r2
- Licenças do Microsoft Defender for Endpoint
- 01 dispositivo com Windows 10 atualizado para homologação das políticas
- Versões do Windows Suportadas
  - Windows 7 SP1 Enterprise
  - Windows 7 SP1 Pro
  - Windows 8.1 Enterpise
  - Windows 8.1 Pro
  - Windows 10, version 1607 or later
  - Windows 10 Enterprise
  - Windows 10 Education
  - Windows 10 Pro
  - Windows 10 Pro Education
- Requisitos de armazenamento de dados e rede, além de configuração:
  - Ao executar o assistente de integração pela primeira vez, você deve escolher onde suas informações relacionadas à proteção avançada contra ameaças do Microsoft defender são armazenadas: na União Européia, no Reino Unido ou no datacenter dos Estados Unidos.
- Conectividade com a Internet:
  - A conectividade com a Internet em dispositivos é necessária diretamente ou por proxy.
  - O sensor ATP do Microsoft defender pode usar uma largura de banda média diária de 5 MB para se comunicar com o serviço de nuvem ATP do Microsoft defender e relatar dados da Cyber. Atividades únicas, como carregamentos de arquivos e coleta de pacote de investigação, não são incluídas nesta largura de banda média diária.
  - O serviço de dados de diagnóstico deve estar habilitado. O serviço é habilitado por padrão no Windows 10.

Itens Fora de Escopo

Microsoft 365

- ❑ Integração com Active Directory do cliente
- ❑ DLP Endpoint para servidores
- ❑ DLP Endpoint para dispositivos não Windows
- ❑ Homologação em dispositivos móveis
- ❑ Configuração de ambiente Intune
- ❑ Configuração de ambiente Endpoint Configuration Manager
- ❑ Configuração de soluções de terceiros para integração com o Defender Endpoint
- ❑ Integração com SIEM
- ❑ Testes de penetração
- ❑ Qualquer outro item que não esteja descrito no escopo ou planejamento do projeto.

Cronograma Macro, Recursos e Custos de Serviço

Tarefa	Horas
Levantamento e Planejamento do Ambiente	20
Execução – Defender Endpoint P1	40
Estabilização, Passagem de conhecimento e documentação	20

Tarefa	Horas
Planejament, Execução, Estabilização, Passagem de conhecimento e documentação – Defender Endpoint P2	32

Local de Execução: Remota

Total = 80 horas / 10 dias + 16 horas de Gestão de Projetos

- ✓ 01 Gerente de Projetos (part-time)
- ✓ 01 Arquiteto de Soluções (part-time)
- ✓ 01 Consultor M365

- ✓ **Obs: Todas as informações acima aqui são meramente estimadas, devendo ser confirmadas para fechamento com propostas técnicas e comercial**

OBRIGADO!

Alexandre Nakano
Arquiteto de Soluções
t-Alexandre.Nakano@brasoftware.com.br